NIAP Government-Industry IT Security Forum

Center for
Information
Security
Technology

March 7, 2001

Robert Williamson
SAIC Common Criteria Testing Laboratory

SAIC
An Employee-Owned Company
www.saic.com

Center for Information Security Technology

- Parent organization for SAIC CCTL
- Two hundred security professionals
- Security technologies,
  - Design,
  - Implementation and
  - Testing
- Common Criteria experience
- Evaluation experience

CENTER FOR
INFORMATION
SECURITY
TECHNOLOGY

Science Applications International Corporation

- **Design, build, deploy and support IT systems**

- **Building process integrates COTS products**

- **Most IT systems require security services to operate as intended**

- **We are heavily involved in identifying security requirements**
  - **functional requirements**
  - **assurance requirements.**

Identifying Customer Security Requirements

- **Functional requirements conflict with security requirements**

- **System security requirements are incompatible**

- **Unclear system security policy**

- **Replace system security requirements with the composite set of product specific security features (reality check)**

SAIC®

An Employee-Owned Company

www.saic.com

Challenges

- **Security specification is tied to**
  - one implementation
  - one set of products
  - one set of solutions

- **Available product security features are not fully compatible with system security requirements**

- **Multiple standards for an organization**

- **Legal requirements**

Observations

- **Source of security specifications – individual procurements**

- **Focus tends to be industry and agency specific**

- **Difficult for customers in different industries and agencies with similar security requirements to benefit from shared security specifications**

Observations

- **IT security solutions and specifications are driven by the security requirements of the IT security context**
  - environment
  - information ownership
  - information sensitivity
  - access
  - type of information technology
  - connectivity

- **And Standards**

Similar Security Requirements Context

Similar security specifications for financial records

- Banks
- Casinos
- Charities
- Churches
- Corporations
- Credit bureaus
- Government credit unions
- Hospitals

- Investment firms
- IRS
- Healthcare providers
- Laboratories
- Office of the Comptroller
- Savings and loans

Towards a Solution

- **Create security specification, based on the IT security context and not the type of business**

- **Create security specifications based on a common language, to facilitate sharing**

- **Share the work**

Common IT security requirements result in common IT security specifications

Shared IT Security Specification

- **Who pays for it?**
- **Who determines appropriate business practices?**
  - **protect subject's information**
  - **limit organizational liability**
- **Who picks the specific requirements?**
- **How is the information distributed?**

Converge on a possible solution

Solution needs to encompass all applicable subsets

- **Bigger than one corporation**

- **Bigger than one agency**

- **Bigger than one industry**

Receive funding from some source

Converge on a possible solution

One candidate – the U.S. Commerce Department.

"The Commerce Department ----- facilitates technology that Americans use in the workplace and home every day; **it supports the development, gathering and transmitting of information essential to competitive business**"
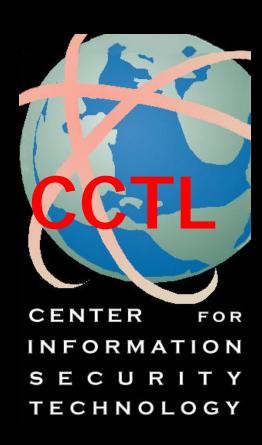
Department of Commerce

- **Already have a program, NIAP, that could be expanded to include industries**

- **Have a funding model**

- **Have a common specification language, the Common Criteria**

- **Have a paradigm to ensure compliance**

SAIC Common Criteria Testing Laboratory

CCTL

CENTER FOR INFORMATION SECURITY TECHNOLOGY

Contact
Tammy Compton
tammy.s.compton@saic.com
(410)953-6832

Robert Williamson
robert.l.williamson.jr@saic.com
(410)953-6819